PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 7 : G07F 7/10

A1

(11) Internationale Veröffentlichungsnummer: **WO 00/16272**

(43) Internationales Veröffentlichungsdatum: 23. März 2000 (23.03.00)

(21) Internationales Aktenzeichen: PCT/EP99/06580

(22) Internationales Anmeldedatum: 7. September 1999 (07.09.99)

(30) Prioritätsdaten:
198 41 676.8 11. September 1998 (11.09.98) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: GIESECKE & DEVRIENT GMBH [DE/DE]; Prinzregentenstrasse 159, D–81677 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: VATER, Harald [DE/DE]; An den Schulgärten 23, D–35398 Gießen (DE). DREXLER, Hermann [DE/DE]; Oberländerstrasse 5a, D–81371 München (DE).

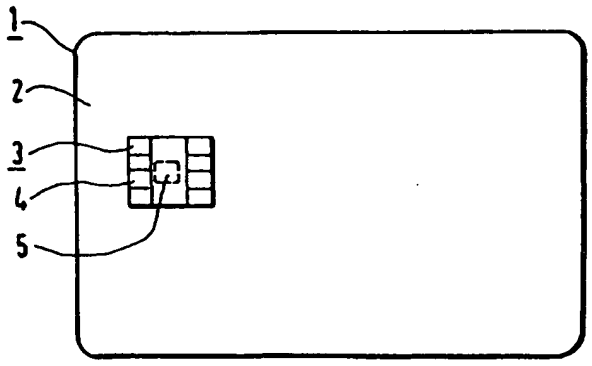
(74) Anwalt: KLUNKER, SCHMITT–NILSON, HIRSCH; Winzererstrasse 106, D–81677 München (DE).

(81) Bestimmungsstaaten: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO Patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht
Mit internationalem Recherchenbericht.

(54) Title: ACCESS–PROTECTED DATA CARRIER

(54) Bezeichnung: ZUGRIFFSGESCHÜTZTER DATENTRÄGER



(57) Abstract

The invention relates to a data carrier, comprising a semiconductor chip (5) with at least one memory. An operating programme which is capable of performing at least one operation (h) is filed in the memory. In order to prevent unauthorised access to the data (x) that is processed with said operation (h), both this data and the operation (h) itself are defamiliarised. The defamiliarisation of the data (x) and the defamiliarisation of the operation (h) are co–ordinated in such a way that the either the output data (y) of the non–defamiliarised operation (h) are produced with the defamiliarised operation (h_{R1R}, h_{R1R2}) or defamiliarised output data ($y \otimes R_2$) from which the output data (y) can be determined.

(57) Zusammenfassung

Die Erfindung betrifft einen Datenträger mit einem Halbleiterchip (5), der wenigstens einen Speicher aufweist. In dem Speicher ist ein Betriebsprogramm abgelegt, das in der Lage ist, wenigstens eine Operation (h) durchzuführen. Um einen unberechtigten Zugriff auf die mit der Operation (h) verarbeiteten Daten (x) zu verhindern, werden sowohl diese Daten als auch die Operation (h) selbst verfremdet. Die Verfremdung der Daten (x) und der Operation (h) ist dabei so aufeinander abgestimmt, daß mit der verfremdeten Operation (h_{R1R}, h_{R1R2}) entweder die Ausgangsdaten (y) der nicht verfremdeten Operation (h) erzeugt werden, oder verfremdete Ausgangsdaten (y o R_2), aus denen die Ausgangsdaten (y) ermittelbar sind.

Zugriffsgeschützter Datenträger

Die Erfindung betrifft einen Datenträger, der einen Halbleiterchip aufweist, in dem geheime Daten abgespeichert sind. Insbesondere betrifft die Erfindung eine Chipkarte.

Datenträger die einen Chip enthalten, werden in einer Vielzahl von unterschiedlichen Anwendungen eingesetzt, beispielsweise zum Durchführen von Finanztransaktionen, zum Bezahlen von Waren oder Dienstleistungen, oder als Identifikationsmittel zur Steuerung von Zugangs- oder Zutrittskontrollen. Bei allen diesen Anwendungen werden innerhalb des Chips des Datenträgers in der Regel geheime Daten verarbeitet, die vor dem Zugriff durch unberechtigte Dritte geschützt werden müssen. Dieser Schutz wird unter anderem dadurch gewährleistet, daß die inneren Strukturen des Chips sehr kleine Abmessungen aufweisen und daher ein Zugriff auf diese Strukturen mit dem Ziel, Daten, die in diesen Strukturen verarbeitet werden, auszuspähen, sehr schwierig ist. Um einen Zugriff weiter zu erschweren, kann der Chip in eine sehr fest haftende Masse eingebettet werden, bei deren gewaltsamer Entfernung das Halbleiterplättchen zerstört wird oder zumindest die darin gespeicherten geheimen Daten vernichtet werden. Ebenso ist es auch möglich, das Halbleiterplättchen bereits bei dessen Herstellung mit einer Schutzschicht zu versehen, die nicht ohne Zerstörung des Halbleiterplättchens entfernt werden kann.

Mit einer entsprechenden technischen Ausrüstung, die zwar extrem teuer aber dennoch prinzipiell verfügbar ist, könnte es einem Angreifer möglicherweise gelingen, die innere Struktur des Chips freizulegen und zu untersuchen. Das Freilegen könnte beispielsweise durch spezielle Ätzverfahren oder durch einen geeigneten Abschleifprozeß erfolgen. Die so freigelegten

Strukturen des Chips, wie beispielsweise Leiterbahnen, könnten mit Mikrosonden kontaktiert oder mit anderen Verfahren untersucht werden, um die Signalverläufe in diesen Strukturen zu ermitteln. Anschließend könnte versucht werden, aus den detektierten Signalen geheime Daten des Datenträgers, wie z.B. geheime Schlüssel zu ermitteln, um diese für Manipulationszwecke einzusetzen. Ebenso könnte versucht werden, über die Mikrosonden die Signalverläufe in den freigelegten Strukturen gezielt zu beeinflussen.

Der Erfindung liegt die Aufgabe zugrunde, geheime Daten, die in dem Chip eines Datenträgers vorhanden sind, vor unberechtigtem Zugriff zu schützen.

Diese Aufgabe wird durch die Merkmalskombinationen der Ansprüche 1 und 9 gelöst.

Die erfindungsgemäße Lösung zielt im Gegensatz zum Stand der Technik nicht darauf ab, ein Freilegen der internen Strukturen des Chips und ein Anbringen von Mikrosonden zu verhindern. Es werden stattdessen Maßnahmen getroffen, die es einem potientellen Angreifer erschweren, aus den gegebenenfalls abgehörten Signalverläufen Rückschlüsse auf geheime Informationen zu schließen. Diese Maßnahmen bestehen erfindungsgemäß darin, sicherheitsrelevante Operationen so zu manipulieren, daß die bei der Durchführung dieser sicherheitsrelevanten Operationen verwendeten Geheimdaten nicht ohne Hinzunahme weiterer geheimer Informationen ermittelbar sind. Hierzu werden die sicherheitsrelevanten Operationen vor ihrer Ausführung mit Hilfe geeigneter Funktionen verfremdet oder verfälscht. Um insbesondere eine statistische Auswertung bei mehrfacher Ausführung der sicherheitsrelevanten Operationen zu erschweren oder gar unmöglich zu machen, fließt in die Verfremdungsfunktion eine Zufallkomponente ein.

Dies hat zur Folge, daß ein Angreifer aus gegebenenfalls abgehörten Datenströmen die Geheimdaten nicht ermitteln kann.

Die sicherheitsrelevante Operation wird im folgenden von der Funktion h repräsentiert, die Eingangsdaten x auf Ausgangsdaten y abbildet, d.h. $y = h(x)$. Um ein Ausspähen der geheimen Eingangsdaten x zu verhindern, wird gemäß der Erfindung eine verfremdete Funktion h_{R1R2} ermittelt, so daß gilt

$$y \otimes R_2 = h_{R1R2}(x \otimes R_1).$$

Die sicherheitsrelevante Operation wird nunmehr mittels der verfremdeten Funktion h_{R1R2} durchgeführt, deren Eingangsdaten nicht die echten Geheimdaten x sind, sondern verfremdete Geheimdaten $x \otimes R_1$, die durch Verknüpfen der echten Geheimdaten x mit einer Zufallszahl R_1 erzeugt wurden. Ohne Kenntnis der Zufallszahl R_1 können die echten Geheimdaten x aus den verfremdeten Geheimdaten $x \otimes R_1$ nicht ermittelt werden. Als Ergebnis der Anwendung der verfremdeten Funktion h_{R1R2} auf die verfremdeten Geheimdaten $x \otimes R_1$ erhält man verfremdete Ausgangsdaten $y \otimes R_2$. Aus den verfremdeten Ausgangsdaten $y \otimes R_2$ lassen sich durch eine geeignete Verknüpfung die Ausgangsdaten y ermitteln. Vor jeder erneuten Durchführung der sicherheitsrelevanten Funktion können neue Zufallszahlen R_1 und R_2 vorgegeben werden, aus denen jeweils eine neue verfremdete Funktion h_{R1R2} ermittelt wird. Alternativ dazu können mehrere verfremdete Funktionen h_{R1R2} fest abgespeichert sein, von denen vor Durchführung der sicherheitsrelevanten Operation jeweils eine zufällig ausgewählt wird. Dabei ist es besonders vorteilhaft zwei Funktionen h_{R1R2} und $h_{R1'R2'}$ zu verwenden, bei denen die Zufallszahlen R'_1 und R'_2 die bzgl der für die Verfremdung gewählten Verknüpfungsart inversen Werte der Zufallszahlen R_1 und R_2 sind. In einer weiteren Variante können die Zufallszahlen R_1 und R_2 auch gleich sein.

Insbesondere können die Zufallszahlen R_1 und R_2 statistisch unabhängig gewählt werden, so daß es keine Korrelation zwischen Ein- und Ausgangsdaten gibt, die für einen Angriff verwendet werden können.

Werden vor oder nach der hier betrachteten sicherheitsrelevanten Operation h noch weitere Operationen abgearbeitet, so können die Zufallszahlen R_1 und R_2 auch zur Verfremdung der mit den weiteren Operationen bearbeiteten Daten benützt werden.

Besonders vorteilhaft läßt sich die erfindungsgemäße Lösung bei sicherheitsrelevanten Operationen einsetzen, die nichtlineare Funktionen beinhalten. Bei nichtlinearen Funktionen können bereits bekannte Schutzmaßnahmen, die auf einer Verfremdung der Geheimdaten vor der Ausführung der Funktionen basieren, nicht angewendet werden. Die bekannten Schutzmaßnahmen setzten nämlich voraus, daß die Funktionen linear bezüglich der Verfremdungsoperationen sind, damit die Verfremdung nach Ausführung der Funktionen wieder rückgängig gemacht werden kann. Bei der erfindungsgemäßen Lösung werden aber nicht nur die Geheimdaten verfälscht oder verfremdet, sondern auch die sicherheitsrelevanten Operationen, die die Geheimdaten verarbeiten. Die Verfremdung der Geheimdaten und der sicherheitsrelevanten Operationen werden dabei so aufeinander abgestimmt, daß aus den verfremdeten Geheimdaten nach Durchführung der sicherheitsrelevanten Operationen die echten Geheimdaten abgeleitet werden können. Die Abstimmung zwischen der Verfremdung der Geheimdaten und der sicherheitsrelevanten Operationen läßt sich besonders einfach realisieren, wenn die sicherheitsrelevanten Operationen in Form von Tabellen, sogenannten Look-up-tables, realisiert sind. In den genannten Tabellen ist jedem Eingangswert x ein Ausgangswert y zugeordnet. Die Ausführung der durch die

Tabellen realisierten Funktionen erfolgt durch Nachschlagen der zu den jeweiligen Eingangswerten x gehörigen Ausgangswerte y.

Die Erfindung wird nachstehend anhand der in den Figuren dargestellten Ausführungsformen erläutert. Es zeigen:

Fig. 1 eine Chipkarte in Aufsicht,

Fig. 2 einen stark vergrößerten Ausschnitt des Chips der in Fig. 1 dargestellten Chipkarte in Aufsicht,

Fig. 3a, 3b, 3c und 3d
Darstellungen von Look-up-tables.

In Fig. 1 ist als ein Beispiel für den Datenträger eine Chipkarte 1 dargestellt. Die Chipkarte 1 setzt sich aus einem Kartenkörper 2 und einem Chipmodul 3 zusammen, das in eine dafür vorgesehene Aussparung des Kartenkörpers 2 eingelassen ist. Wesentliche Bestandteile des Chipmoduls 3 sind Kontaktflächen 4, über die eine elektrische Verbindung zu einem externen Gerät hergestellt werden kann und ein Chip 5, der mit den Kontaktflächen 4 elektrisch verbunden ist. Alternativ oder zusätzlich zu den Kontaktflächen 4 kann auch eine in Fig. 1 nicht dargestellte Spule oder ein anderes Übertragungmittel zur Herstellung einer Kommunikationsverbindung zwischen dem Chip 5 und einem externen Gerät vorhanden sein.

In Fig. 2 ist ein stark vergrößerter Ausschnitt des Chips 5 aus Fig. 1 in Aufsicht dargestellt. Das besondere der Fig. 2 liegt darin, daß die aktive Oberfläche des Chips 5 dargestellt ist, d.h. sämtliche Schichten, die im allgemeinen die aktive Schicht des Chips 5 schützen, sind in Fig. 2 nicht dargestellt. Um

Informationen über die Signalverläufe im Inneren des Chips zu erhalten, können beispielsweise die freigelegten Strukturen 6 mit Mikrosonden kontaktiert werden. Bei den Mikrosonden handelt es sich um sehr dünne Nadeln, die mittels einer Präzisions-Positioniereinrichtung mit den freigelegten Strukturen 6, beispielsweise Leiterbahnen in elektrischen Kontakt gebracht werden. Die mit den Mikrosonden aufgenommenen Signalverläufe werden mit geeigneten Meß- und Auswerteeinrichtungen weiterverarbeitet mit dem Ziel, Rückschlüsse auf geheime Daten des Chips schließen zu können.

Mit der Erfindung wird erreicht, daß ein Angreifer auch dann, wenn es ihm gelungen sein sollte, die Schutzschicht des Chips 5 ohne Zerstörung des Schaltkreises zu entfernen und die freigelegten Strukturen 6 des Chips 5 mit Mikrosonden zu kontaktieren oder auf andere Weise abzuhören nur sehr schwer oder gar nicht Zugang zu insbesondere geheimen Daten des Chips erlangt. Selbstverständlich greift die Erfindung auch dann, wenn ein Angreifer auf andere Art und Weise Zugang zu den Signalverläufen des Chips 5 erlangt.

Die Figuren 3a, 3b, 3c und 3d zeigen einfache Beispiele für Look-up-tables, bei denen sowohl die Eingangs- als auch die Ausgangsdaten jeweils eine Länge von 2 bit haben. Alle Tabellenwerte sind als binäre Daten dargestellt. In der ersten Zeile sind jeweils die Eingangsdaten x und in der zweiten Zeile die jeweils spaltenweise zugeordneten Ausgangsdaten y dargestellt.

In Figur 3a ist ein Look-up-table für die nicht verfremdete Funktion h dargestellt. Der Figur 3a ist entnehmbar, daß dem Eingangswert x = 00 der Ausgangswert h (x) = 01 zugeordnet ist, dem Eingangswert 01 der Ausgangswert 11, dem Eingangswert 10 der Ausgangswert 10 und dem Eingangswert 11 der Ausgangswert 00. Die Look-up-table gemäß Figur 3a repräsentiert

eine nichtlineare Funktion h, die im Rahmen einer sicherheitsrelevanten Operation ausgeführt werden soll. Im Rahmen der Erfindung wird bei der Durchführung der sicherheitsrelevanten Operation jedoch nicht die in Figur 3a abgebildete Look-up-table selbst verwendet, sondern aus dieser Look-up-table wird gemäß den Figuren 3b, 3c und 3d eine verfremdete Look-up-table abgeleitet.

In Figur 3b ist ein Zwischenschritt der Ermittlung der verfremdeten Look-up-table dargestellt. Die Look-up-table gemäß Figur 3b wurde aus der Look-up-table gemäß Figur 3a erzeugt, indem jeder Wert der ersten Zeile der Tabelle aus Figur 3a mit der Zufallszahl $R_1 = 11$ EXOR verknüpft wurde. So ergib die EXOR-Verknüpfung des Wertes 00 der ersten Zeile und ersten Spalte der Tabelle aus Figur 3a mit der Zahl 11 den Wert 11, der nunmehr das Element der ersten Zeile und ersten Spalte der Tabelle der Figur 3b darstellt. Entsprechend werden die restlichen Werte der ersten Zeile der in Figur 3b dargestellten Tabelle aus den Werten der ersten Zeile der in Figur 3a dargestellten Tabelle und der Zufallszahl $R_1 = 11$ ermittelt. Die in Figur 3b dargestellte Tabelle könnte bereits als verfremdete Look-up-table zur Verarbeitung von ebenfalls mit der Zufallszahl $R_1 = 11$ verfremdeten Geheimdaten eingesetzt werden. Das Ergebnis wäre dann jeweils die in Zeile 2 der Tabelle aus Figur 3b abzulesenden Klartextwerte.

Üblicherweise ordnet man die einzelnen Spalten einer Look-up-table nach aufsteigenden Eingangsdaten x an. Eine durch entsprechende Umsortierung der Tabelle in Figur 3b ermittelte Tabelle ist in Figur 3c dargestellt.

Falls die Tabelle gemäß Figur 3c noch weiter verfremdet werden soll bzw. als Ausgangswerte keine Klartextwerte sondern ebenfalls verfremdete Werte liefern soll, wird eine weitere EXOR-Operation mit einer weiteren Zufallszahl R_2 angewendet.

In Figur 3d ist das Ergebnis der Anwendung dieser weiteren EXOR-Operation dargestellt. Bei dieser Operation werden jeweils die Elemente der zweiten Zeile der Tabelle gemäß Figur 3c mit der Zufallszahl $R_2 = 10$ EXOR verknüpft. Das Element in der zweiten Zeile und der ersten Spalte der Tabelle gemäß Figur 3d entsteht also durch EXOR-Verknüpfung des Elements in der zweiten Zeile und ersten Spalte der Tabelle gemäß Figur 3c der Zufallszahl $R_2 = 10$. Entsprechend werden die weiteren Elemente der zweiten Zeile der Tabelle gemäß Figur 3d gebildet. Die erste Zeile der Tabelle gemäß Figur 3d wird von Figur 3c unverändert übernommen.

Mit der in Figur 3d abgebildeten Tabelle können aus verfremdeten Eingangsdaten ebenfalls verfremdete Ausgangsdaten ermittelt werden. Die so ermittelten verfremdeten Ausgangsdaten können weiteren Operationen zugeführt werden, mit denen verfremdete Daten verarbeitet werden sollen oder es können daraus durch EXOR-Verknüpfung mit der Zufallszahl $R_2 = 10$ Klartextdaten ermittelt werden.

Durch Verwendung der in Figur 3d dargestellten Tabelle ist es möglich, auch nichtlineare Operationen mit verfremdeten Geheimdaten durchzuführen und diese Geheimdaten vor unberechtigtem Zugriff zu schützen. Weiterhin werden auch die sicherheitsrelvanten Operationen selbst vor unberechtigtem Zugriff geschützt, da bei jeder Durchführung der Operationen andersartig

verfremdete Funktionen eingesetzt werden können und man selbst dann, wenn man die verfremdeten Funktionen ermitteln könnte, nicht auf die sicherheitsrelevanten Operationen selbst schließen kann. Nach Umwandlung in Klartext liefern aber sowohl die ursprünglichen sicherheitsrelevanten Operationen als auch die mit Hilfe von verfremdeten Funktionen durchgeführten Operationen identische Ergebnisse. So ergibt beispielsweise ein Eingangswert 00 gemäß der Tabelle in Figur 3a einen Ausgangswert 01. Um zu überprüfen, ob die in Figur 3d dargestellte verfremdete Tabelle den gleichen Ausgangswert liefert, muß der Eingangswert 00 zunächst mit der Zufallszahl $R_1 = 11$ EXOR verknüpft werden. Als Ergebnis dieser Verknüpfung erhält man den Wert 11. Laut der Tabelle aus Figur 3d ergibt ein Eingangswert 11 einen Ausgangswert von ebenfalls 11. Um aus diesem Ausgangswert den Klartext zu ermitteln, ist der Ausgangswert mit der Zufallszahl $R_2 = 10$ EXOR zu verknüpfen. Als Ergebnis dieser Verknüpfung erhält man den Wert 01, der mit dem mit Hilfe der in Figur 3a abgebildeten Tabelle ermittelten Werte exakt übereinstimmt.

Die Verfremdung der sicherheitsrelevanten Operationen bzw. der Eingangswerte kann nicht nur durch EXOR-Verknüpfung erzeugt werden, sondern auch durch andere geeignete Verknüpfungsarten, beispielsweise durch eine modulare Addition. Desweiteren ist die Erfindung nicht auf die Anwendung von nichtlinearen Funktionen begrenzt, die mittels der Look-up-tables repräsentiert werden. Es können vielmehr beliebige nichtlineare und auch lineare Funktionen zum Einsatz kommen, für die eine geeignete verfremdete Funktion ermittelbar ist.

Patentansprüche

1. Datenträger mit einem Halbleiterchip (5) der wenigstens einen Speicher aufweist, in dem ein Betriebsprogramm abgelegt ist, das in der Lage ist, wenigstens eine Operation (h) auszuführen, wobei für die Ausführung der Operation (h) Eingangsdaten (x) benötigt werden und bei der Ausführung der Operation (h) Ausgangsdaten (y) erzeugt werden, **dadurch gekennzeichnet,** daß

- die Operation (h) vor ihrer Ausführung verfremdet wird,
- die verfremdete Operation (h_{R1}) mit verfremdeten Eingangsdaten ($x \otimes R_1$) ausgeführt wird und
- die Verfremdung der Operation (h) und der Eingangsdaten (x) so aufeinander abgestimmt werden, daß die Ausführung der verfremdeten Operation (h_{R1}) mit verfremdeten Eingangsdaten ($x \otimes R_1$) Ausgangsdaten (y) ergibt, die mit den Ausgangsdaten (y) identisch sind, die bei Ausführung der nicht verfremdeten Operation (h) mit nicht verfremdeten Eingangsdaten (x) ermittelt werden.

2. Datenträger nach Anspruch 1, **dadurch gekennzeichnet,** daß in die Ermittlung der verfremdeten Operation (h_{R1}) und der verfremdeten Eingangsdaten ($x \otimes R_1$) wenigstens eine Zufallszahl (R_1) eingeht.

3. Datenträger nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** daß die Ermittlung der verfremdeten Operation (h_{R1}) und der verfremdeten Eingangsdaten ($x \otimes R_1$) unter Zuhilfenahme von EXOR-Verknüpfungen verfolgt.

4. Datenträger nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** daß die verfremdete Operation (h_{R1}) vorab im Datenträger fest eingespeichert wird.

5. Datenträger nach Anspruch 4, **dadurch gekennzeichnet,** daß wenigstens zwei verfremdete Operationen (h_{R1}, h_{R1}') vorab in Datenträger fest eingespeichert werden und dann, wenn eine verfremdete Operation ausgeführt werden soll, aus den gespeicherten verfremdeten Operationen (h_{R1}, h_{R1}') eine zufallsbedingt ausgewählt wird.

6. Datenträger nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet,** daß die verfremdete Operation (h_{R1}) vor ihrer Ausführung jeweils neu berechnet wird und für diese Berechnung die wenigstens eine Zufallszahl (R_1) neu ermittelt wird.

7. Datenträger nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** daß die Operation (h) durch eine im Datenträger gespeicherte Tabelle realisiert ist, die eine Zuordnung zwischen den Eingangsdaten (x) und den Ausgangsdaten (y) herstellt.

8. Datenträger nach Anspruch 7, **dadurch gekennzeichnet,** daß die Verfremdung der in der Tabelle enthaltenen Eingangsdaten (x) durch Verknüpfung mit der wenigstens einen Zufallszahl (R1) erfolgt.

9. Datenträger mit einem Halbleiterchip (5) der wenigstens einen Speicher aufweist, in dem ein Betriebsprogramm abgelegt ist, das in der Lage ist, wenigstens eine Operation (h) auszuführen, wobei für die Ausführung der Operation (h) Eingangsdaten (x) benötigt werden und bei der Ausführung

der Operation (h) Ausgangsdaten (y) erzeugt werden, **dadurch gekennzeichnet,** daß

- die Operation (h) vor ihrer Ausführung verfremdet wird,
- die verfremdete Operation (h_{R1}) mit verfremdeten Eingangsdaten ($x \otimes R_1$) ausgeführt wird,
- die Verfremdung der Operation (h) und der Eingangsdaten (x) so aufeinander abgestimmt werden, daß die Ausführung der verfremdeten Operation (h_{R1R2}) mit verfremdeten Eingangsdaten ($x \otimes R_1$) Ausgangsdaten ($y \otimes R_2$) ergibt, die gegenüber den Ausgangsdaten (y), die bei Ausführung der nicht verfremdeten Operation (h) mit nicht verfremdeten Eingangsdaten (x) ermittelt werden, verfremdet sind und
- aus den verfremdeten Ausgangsdaten ($y \otimes R_2$) unter Zuhilfenahme vonDaten (R_2), die für die Verfremdung der Operation (h) verwendet wurden, die nicht verfremdeten Ausgangsdaten (y) ermittelbar sind.

10. Datenträger nach Anspruch 9, **dadurch gekennzeichnet,** daß in die Ermittlung der verfremdeten Eingangsdaten ($x \otimes R_1$) wenigstens eine Zufallszahl (R_1) eingeht und daß in die Ermittlung der verfremdeten Operationen (h_{R1R2}) wenigstens zwei Zufallszahlen (R_1, R_2) eingehen.

11. Datenträger nach einem der Ansprüche 9 oder 10, **dadurch gekennzeichnet,** daß die Ermittlung der verfremdeten Operation ($h_{R1, R2}$) und der verfremdeten Eingangsdaten ($x \otimes R_1$) unter Zuhilfenahme von EXOR-Verknüpfungen erfolgt.

12. Datenträger nach einem der Ansprüche 9 bis 11, **dadurch gekennzeichnet,** daß die verfremdete Operation (h_{R1R2}) vorab im Datenträger fest eingespeichert wird.

13. Datenträger nach Anspruch 12, **dadurch gekennzeichnet,** daß wenigstens zwei verfremdete Operationen (h_{R1R2}, $h_{R1'R2'}$) vorab in Datenträger fest eingespeichert werden und dann, wenn eine verfremdete Operation ausgeführt werden soll, aus den gespeicherten verfremdeten Operationen (h_{R1R2}, $h_{R1'R2'}$) eine zufallsbedingt ausgewählt wird.

14. Datenträger nach Anspruch 13, **dadurch gekennzeichnet,** daß die Zufallszahlen (R_1, R_2) mit denen die erste verfremdete Operation (h_{R1R2}) ermittelt wird bezüglich der Verknüpfung, die bei der Ermittlung der verfremdeten Operationen (h_{R1R2} ,$h_{R1'R2'}$) verwendet wird, invers sind zu den Zufallszahlen (R_1', R_2'), mit denen die zweite verfremdete Operation ($h_{R1'R2'}$) ermittelt wird.

15. Datenträger nach einem der Ansprüche 9 bis 11, **dadurch gekennzeichnet,** daß die verfremdete Operation (h_{R1R2}) vor ihrer Ausführung jeweils neu berechnet wird und für diese Berechnung die Zufallszahlen (R_1, R_2) neu ermittelt werden.

16. Datenträger nach einem der Ansprüche 9 bis 15, **dadurch gekennzeichnet,** daß die Operation (h) durch eine im Datenträger gespeicherte Tabelle realisiert ist, die eine Zuordnung zwischen den Eingangsdaten (x) und den Ausgangsaten (y) herstellt.

17. Datenträger nachAnspruch 16, **dadurch gekennzeichnet,** daß die Verfremdung der in der Tabelle enthaltenen Eingangsdaten (x) durch Verknüpfung mit der wenigstens einen Zufallszahl (R1) erfolgt und die Verfremdung der in der Tabelle enthaltenen Ausgangsdaten (y) durchVerknüpfung mit der wenigstens einen weiteren Zufallszahl (R2) erfolgt.

18. Datenträger nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, daß es sich bei der Operation (h) um eine bezüglich der für die Verfremdung der Operation (h) eingesetzten Verknüpfung nichtlineare Operation handelt.

FIG.1

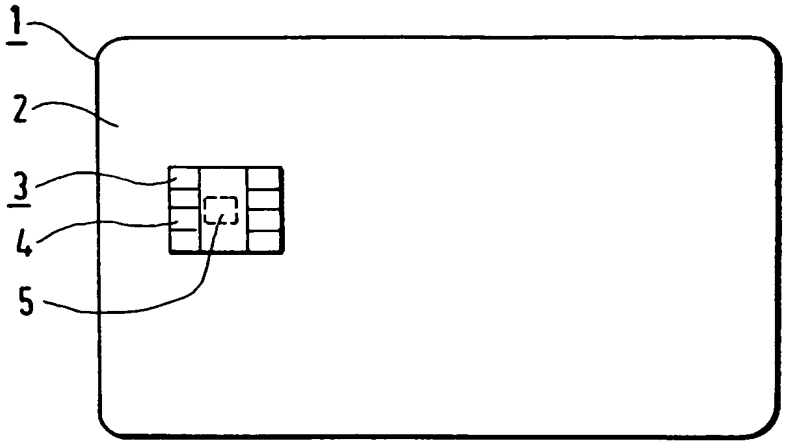


FIG.2

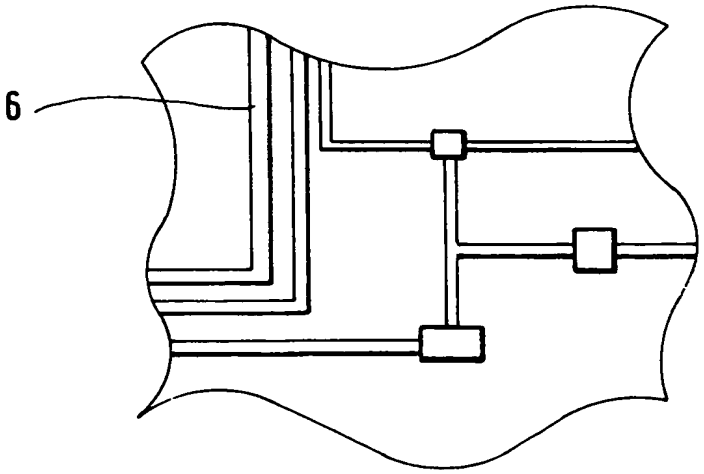


FIG.3A

x	00	01	10	11
h(x)	01	11	10	00

FIG.3B

x	11	10	01	00
$h_{R1}(x)$	01	11	10	00

FIG.3C

x	00	01	10	11
$h_{R1}(x)$	00	10	11	01

FIG.3D

x	00	01	10	11
$h_{R1\,R2}(x)$	10	00	01	11

INTERNATIONAL SEARCH REPORT

International Application No
/EP 99/06580

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 743 775 A (FRANCE TELECOM ;POSTE (FR)) 20 November 1996 (1996-11-20) page 2, line 9 - line 16 page 5, line 33 -page 6, line 16 page 7, line 19 - line 23	1-4,9,11
A	US 4 974 193 A (BEUTELSPACHER ALBRECHT ET AL) 27 November 1990 (1990-11-27) column 2, line 49 -column 3, line 48; claim 1 figure 5	1-4,9,11

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 November 1999	01/12/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	de Ronde, J.

Form PCT/ISA/210 (second sheet) (July 1992)

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0743775 A	20-11-1996	FR 2734435 A	22-11-1996
		DE 69600143 D	19-02-1998
		DE 69600143 T	07-05-1998
US 4974193 A	27-11-1990	DE 3706955 A	15-09-1988
		AT 105642 T	15-05-1994
		DE 3889481 D	16-06-1994
		EP 0281057 A	07-09-1988
		ES 2051780 T	01-07-1994
		JP 63228353 A	22-09-1988

TENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Assistant Commissioner for Patents
United States Patent and Trademark Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 19 May 2000 (19.05.00)	
International application No. PCT/EP99/06580	**Applicant's or agent's file reference** K 49 779/7 ch
International filing date (day/month/year) 07 September 1999 (07.09.99)	**Priority date** (day/month/year) 11 September 1998 (11.09.98)
Applicant VATER, Harald et al	

1. The designated Office is hereby notified of its election made:

   [X] in the demand filed with the International Preliminary Examining Authority on:

   10 April 2000 (10.04.00)

   [ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

   [ ] was not

   made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland**	Authorized officer Juan Cruz
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

To:

KLUNKER, SCHMITT-NILSON, HIRSCH
Winzererstrasse 106
D-80797 München
ALLEMAGNE

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

Date of mailing (day/month/year) 16 June 2000 (16.06.00)	
Applicant's or agent's file reference K 49 779/7 ch	**IMPORTANT NOTIFICATION**
International application No. PCT/EP99/06580	**International filing date** (day/month/year) 07 September 1999 (07.09.99)

1. The following indications appeared on record concerning:

☐ the applicant ☐ the inventor ☒ the agent ☐ the common representative

Name and Address	State of Nationality	State of Residence
KLUNKER, SCHMITT-NILSON, HIRSCH Winzererstrasse 106 D-81677 München Germany		
	Telephone No. 089 30 77 410	
	Facsimile No. 089 30 77 41 41	
	Teleprinter No.	

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

☐ the person ☐ the name ☒ the address ☐ the nationality ☐ the residence

Name and Address	State of Nationality	State of Residence
KLUNKER, SCHMITT-NILSON, HIRSCH Winzererstrasse 106 D-80797 München Germany		
	Telephone No. 089 30 77 410	
	Facsimile No. 089 30 77 41 41	
	Teleprinter No.	

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

☒ the receiving Office
☐ the International Searching Authority
☒ the International Preliminary Examining Authority
☐ the designated Offices concerned
☒ the elected Offices concerned
☐ other:

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland**	Authorized officer G. Bähr
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

09/763621
Translation
5080

RECEIVED
JUN 4 2001
Technology Center 2100

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference K 49 779/7 ch	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/EP99/06580	International filing date (*day/month/year*) 07 September 1999 (07.09.99)	Priority date (*day/month/year*) 11 September 1998 (11.09.98)
International Patent Classification (IPC) or national classification and IPC G07F 7/10		
Applicant GIESECKE & DEVRIENT GMBH		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of _____ sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
10 April 2000 (10.04.00)	19 May 2000 (19.05.2000)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/EP99/06580

I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

☐ the international application as originally filed.

☒ the description, pages 1-9, as originally filed,
pages _____, filed with the demand,
pages _____, filed with the letter of _____
pages _____, filed with the letter of _____

☒ the claims, Nos. 1-18, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. _____, filed with the letter of _____
Nos. _____, filed with the letter of _____

☒ the drawings, sheets/fig 1/2-2/2, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____
sheets/fig _____, filed with the letter of _____

2. The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

V. **Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	1-18	YES
	Claims		NO
Inventive step (IS)	Claims	1-18	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-18	YES
	Claims		NO

2. Citations and explanations

This report makes reference to the following documents:

D1 EP-A-0 743 775 (FRANCE TELECOM; POSTE (FR)) 20 November 1996 (1996-11-20)

D2 US-A-4 974 193 (BEUTELSPACHER ALBRECHT ET AL) 27 November 1990 (1990-11-27).

A data carrier with the features of the preamble of independent Claims 1 and 9 is considered to be the closest prior art.

The search report citations D1 and D2 relate only to the technical background and do not go beyond the preamble of independent Claims 1 and 9. None of the documents discloses the feature essential to the invention, namely that the operation h is made unfamiliar before being carried out. Moreover, none of the documents suggests the feature, essential to the invention, of Claim 1, of co-ordinating the defamiliarisation of the operation h -> h' and the input data x -> x' to each other in such a manner that h(x) = h'(x'). The solution according to Claim 9 is based on the same inventive concept, with h(x) = h''(h'(x')).

In this way the problem of protecting secret data present in the chip of a data carrier even when signal shapes in the chip are listened to, for example with microprobes, is solved.

No objection can be made with respect to industrial applicability.

Consequently, independent Claims 1 and 9 would appear to meet the criteria stipulated in PCT Article 33(1) concerning novelty, inventive step and industrial applicability. Claims 2-8 and 10-18 relate to advantageous developments and therefore also meet the criteria stipulated.

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

To meet the requirements of PCT Rule 5.1(a)(ii), the document, in relation to which independent Claims 1 and 9 have been delimited, should have been cited. For this purpose, D2, for example, should have been mentioned in the description.

Note: this minor amendment can be made in the regional phase

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

Pursuant to PCT Article 6, there should be no doubts about the category of the independent claims. Claims 1 and 9 relate to a device. However, the current wording of the characterising part of the claims in this manner indicates a method and should have been as follows:

- means for defamiliarisation of the operation (h) before it is carried out,
- means for carrying out the defamiliarised ...
- means for co-ordinating the defamiliarisation of the operation (h) and the input data (x) with the result that ...

In addition, Claim 9:

- means for determining the non-defamiliarised output data (y) from the ...

Note: this previously formal objection can be removed in the regional phase.

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts	**WEITERES VORGEHEN**	siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsbericht (Formblatt PCT/IPEA/416)
K 49 779/7 ch		
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	Prioritätsdatum *(Tag/Monat/Tag)*
PCT/EP99/06580	07/09/1999	11/09/1998
Internationale Patentklassification (IPK) oder nationale Klassifikation und IPK		
G07F7/10		
Anmelder		
GIESECKE & DEVRIENT GMBH et al.		

1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationale vorläufigen Prüfung beauftragte Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.

2. Dieser BERICHT umfaßt insgesamt 5 Blätter einschließlich dieses Deckblatts.

   ☐ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

   Diese Anlagen umfassen insgesamt Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

   - I ☒ Grundlage des Berichts
   - II ☐ Priorität
   - III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
   - IV ☐ Mangelnde Einheitlichkeit der Erfindung
   - V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderische Tätigkeit und der gewerbliche Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
   - VI ☐ Bestimmte angeführte Unterlagen
   - VII ☒ Bestimmte Mängel der internationalen Anmeldung
   - VIII ☒ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags	Datum der Fertigstellung dieses Berichts
10/04/2000	19.05.00
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde:	Bevollmächtigter Bediensteter
Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Kampka, A Tel. Nr. +49 89 2399 2244

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/EP99/06580

I. Grundlage des Berichts

1. Dieser Bericht wurde erstellt auf der Grundlage (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigefügt, weil sie keine Änderungen enthalten.*):

Beschreibung, Seiten:

1-9 ursprüngliche Fassung

Patentansprüche, Nr.:

1-18 ursprüngliche Fassung

Zeichnungen, Blätter:

1/2-2/2 ursprüngliche Fassung

2. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

   ☐ Beschreibung, Seiten:
   ☐ Ansprüche, Nr.:
   ☐ Zeichnungen, Blatt:

3. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)):

4. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja:	Ansprüche	1 - 18
	Nein:	Ansprüche	
Erfinderische Tätigkeit (ET)	Ja:	Ansprüche	1 - 18
	Nein:	Ansprüche	
Gewerbliche Anwendbarkeit (GA)	Ja:	Ansprüche	1 - 18
	Nein:	Ansprüche	

2. Unterlagen und Erklärungen

siehe Beiblatt

VII. Bestimmte Mängel der internationalen Anmeldung

Es wurde festgestellt, daß die internationale Anmeldung nach Form oder Inhalt folgende Mängel aufweist:

siehe Beiblatt

VIII. Bestimmte Bemerkungen zur internationalen Anmeldung

Zur Klarheit der Patentansprüche, der Beschreibung und der Zeichnungen oder zu der Frage, ob die Ansprüche in vollem Umfang durch die Beschreibung gestützt werden, ist folgendes zu bemerken:

siehe Beiblatt

Zu Punkt V

Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

Es wird auf die folgenden Dokumente verwiesen:

D1: EP-A-0 743 775 (FRANCE TELECOM ;POSTE (FR)) 20. November 1996 (1996-11-20)
D2: US-A-4 974 193 (BEUTELSPACHER ALBRECHT ET AL) 27. November 1990 (1990-11-27)

Als nächstliegender Stand der Technik wird ein Datenträger mit den Merkmalen des Oberbegriffs der unabhängigen Ansprüche 1 und 9 angesehen.

Die im Recherchenbericht zitierten Dokumente D1 und D2 betreffen nur den technischen Hintergrund und gehen nicht über den Oberbegriff der unabhängigen Ansprüche 1 und 9 hinaus. Keines der Dokumente offenbart das erfindungswesentliche Merkmal, daß die Operation h vor ihrer Ausführung verfremdet wird. Außerdem gibt keines der Dokumente einen Hinweis auf das erfindungswesentliche Merkmal des Anspruches 1, die Verfremdung der Operation h -> h' und der Eingangsdaten x -> x' so aufeinander abzustimmen, daß h(x) = h'(x'). Die Lösung gemäß Anspruch 9 basiert auf demselben erfinderischen Konzept, mit h(x) = h''(h'(x')).

Damit wird die Aufgabe gelöst, geheime Daten, die im Chip eines Datenträgers vorhanden sind, auch dann zu schützen, wenn Signalverläufe im Chip abgehört werden, etwa mit Mikrosonden.

Zur gewerblichen Anwendbarkeit ist nichts einzuwenden.

Somit dürften die unabhängigen Ansprüche 1 und 9 die in Artikel 33(1) PCT genannten Kriterien der Neuheit, erfinderischen Tätigkeit und gewerblichen Anwendbarkeit erfüllen. Die Ansprüche 2 - 8 und 10 - 18 betreffen vorteilhafte Ausgestaltungen und erfüllen daher ebenfalls die genannten Kriterien.

Zu Punkt VII
Bestimmte Mängel der internationalen Anmeldung

Damit die Erfordernisse der Regel 5.1(a)(ii) PCT erfüllt werden, hätte das Dokument zitiert werden sollen, gegenüber dem die unabhängigen Ansprüche 1 und 9 abgegrenzt wurden. Dazu hätte in der Beschreibung z.B. das Dokument D2 angegeben werden können.

Anmerkung: diese kleine Ergänzung kann in der regionalen Phase vorgenommen werden.

Zu Punkt VIII
Bestimmte Bemerkungen zur internationalen Anmeldung

Um die Erfordernisse des Art. 6 PCT zu erfüllen, sollte kein Zweifel hinsichtlich der Kategorie der unabhängigen Ansprüche entstehen. Die Ansprüche 1 und 9 betreffen eine Vorrichtung. Die derzeitige Formulierung des kennzeichnenden Teils der Ansprüche deutet aber eher auf ein Verfahren hin und hätte etwa wie folgt formuliert werden sollen:

- Mittel zur Verfremdung der Operation (h) vor ihrer Ausführung,
- Mittel zur Ausführung der verfremdeten...
- Mittel zur Abstimmung der Verfremdung der Operation (h) und der Eingangsdaten (x), so daß ...

Anspruch 9 zusätzlich:
- Mittel zur Ermittlung der nicht verfremdeten Ausgangsdaten (y) aus den...

Anmerkung: dieser eher formale Einwand kann in der regionalen Phase behoben werden.

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT
AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts	WEITERES VORGEHEN	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5
K 49 779/7 ch		
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	(Frühestes) Prioritätsdatum *(Tag/Monat/Jahr)*
PCT/EP 99/ 06580	07/09/1999	11/09/1998
Anmelder		
GIESECKE & DEVRIENT GMBH et al.		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 2 Blätter.

[X] Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. **Grundlage des Berichts**

   a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

   [ ] Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

   b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

   [ ] in der internationalen Anmeldung in schriftlicher Form enthalten ist.

   [ ] zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

   [ ] Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

   [ ] Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. [ ] **Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen** (siehe Feld I).

3. [ ] **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

4. Hinsichtlich der **Bezeichnung der Erfindung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der **Zusammenfassung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 1

   [ ] wie vom Anmelder vorgeschlagen

   [ ] keine der Abb.

   [X] weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

   [ ] weil diese Abbildung die Erfindung besser kennzeichnet.

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
T/EP 99/06580

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G07F7/10

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G07F G06F H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der Internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 0 743 775 A (FRANCE TELECOM ;POSTE (FR)) 20. November 1996 (1996-11-20) Seite 2, Zeile 9 - Zeile 16 Seite 5, Zeile 33 -Seite 6, Zeile 16 Seite 7, Zeile 19 - Zeile 23	1-4,9,11
A	US 4 974 193 A (BEUTELSPACHER ALBRECHT ET AL) 27. November 1990 (1990-11-27) Spalte 2, Zeile 49 -Spalte 3, Zeile 48; Anspruch 1 Abbildung 5	1-4,9,11

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem Internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem Internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem Internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann nahellegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der Internationalen Recherche	Absendedatum des Internationalen Recherchenberichts
24. November 1999	01/12/1999

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	de Ronde, J.

3